

# PRÁCTICA 1: CONFIDENCIALIDAD

Nicolás González Dobarro

# Índice

PARTE DE WINDOWS.....	3
PARTE A.....	3
1. Inicia sesión con "usu1" y crea una carpeta con esta estructura:.....	3
2. Cifra la carpeta "confidential_usu1".....	3
3. Comprueba los certificados de cifrado de archivo de "usu1".....	4
4. Comprueba los certificados de usuario personales de "usu1".....	4
5. Comprueba que puedes abrir y ver los documentos:.....	5
6. Inicia sesión con el usuario "usu2" y trata de abrir los documentos:.....	5
PARTE B.....	7
PASO 1. Abrir los certificados de usuario desde el panel de control.....	7
PASO 2. Hacer una copia del certificado y de la clave desde el panel de control.....	7
PASO 3. Elegimos la ruta de la copia de seguridad y escribimos la clave.....	8
PASO 4. Así se realizaría la copia de seguridad, ahora tendremos que iniciar sesión con usu2.	8
PASO 5. Una vez tengamos el certificado, lo abrimos y procederemos a su importación.....	9
PASO 6. Seleccionamos el certificado que queremos instalar.....	9
PASO 7. Ahora escribimos la clave privada para descifrar el certificado.....	10
PASO 8. Una vez finalizado, ya tendríamos acceso a la carpeta cifrada de usu1.....	10
PARTE DE LINUX.....	12
PASO 1. Instala el paquete "seahorse-nautilus".....	12
PASO 2. Accede al gestor de contraseñas y claves de Ubuntu.....	12
PASO 3. Crea una nueva clave PGP "clave_usu1" con contraseña "abc123.".....	13
PASO 4. Crea la siguiente estructura de carpetas y documentos en el escritorio:.....	13
PASO 5. Cifra la carpeta usando la clave PGP "clave_usu1". Para ello selecciona la opción de cifrar en un único paquete.....	13
PASO 6. Muestra el fichero .pgp creado.....	13
PASO 7. Inicia sesión con otro usuario "usu2" e intenta descifrar el fichero .pgp.....	14
PASO 8. Vuelve a iniciar sesión con el usuario original "usu1" y descifra el fichero .pgp.....	14

## PARTE DE WINDOWS

### PARTE A

#### 1. Inicia sesión con "usu1" y crea una carpeta con esta estructura:

C:/

-> Carpeta "confidential\_usu1"

-> Documento "confidential.txt" con texto guardado

-> Subcarpeta "imágenes"

-> Imagen "foto\_comprometida.jpg"

```
C:\Windows\System32\cmd.exe

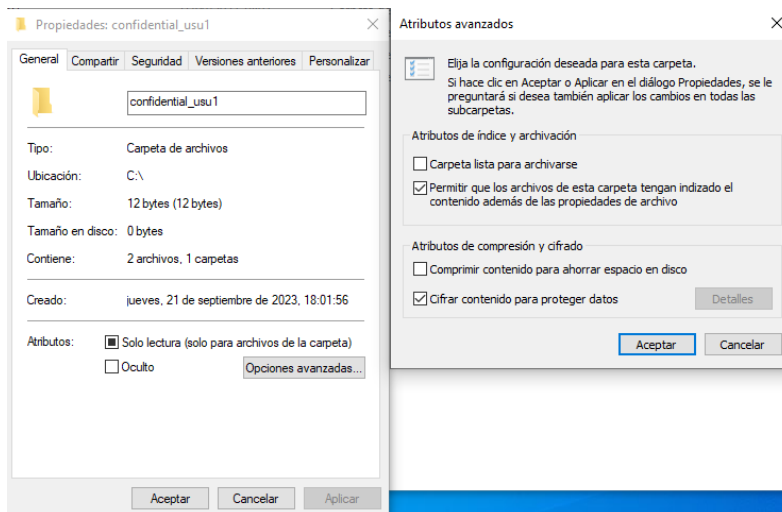
C:\confidential_usu1>dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 26A7-7738

Directorio de C:\confidential_usu1

21/09/2023  18:03    <DIR>          .
21/09/2023  18:03    <DIR>          ..
21/09/2023  18:03                12 confidential.txt
21/09/2023  18:03    <DIR>          imágenes
                1 archivos             12 bytes
                3 dirs  84.593.246.208 bytes libres
```

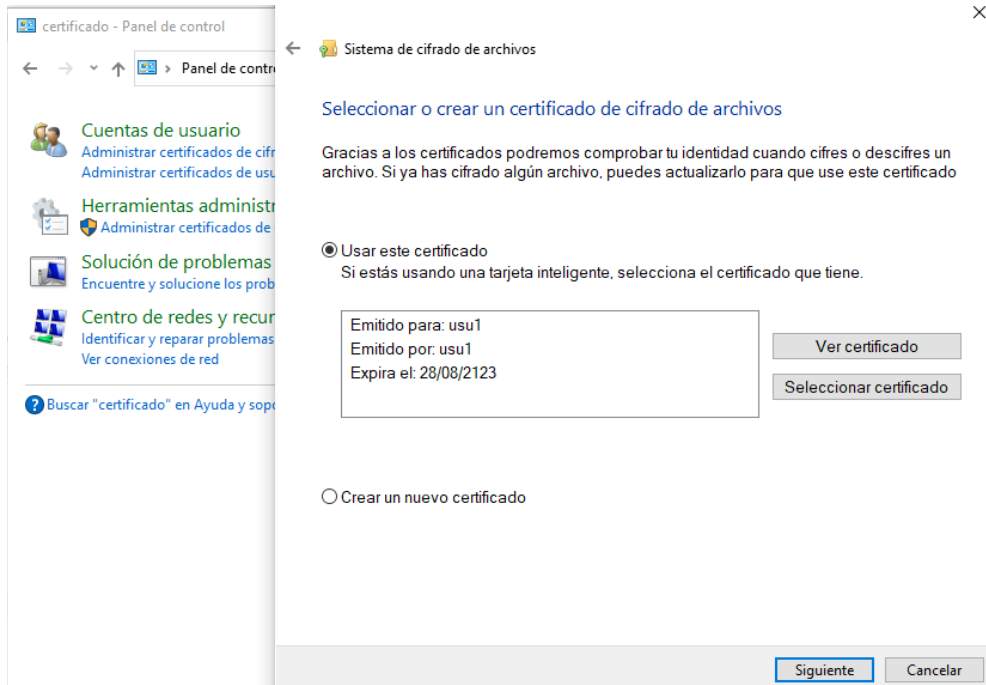
#### 2. Cifra la carpeta "confidential\_usu1"

- Si no tenía instalado ningún certificado de cifrado, se creará uno nuevo.



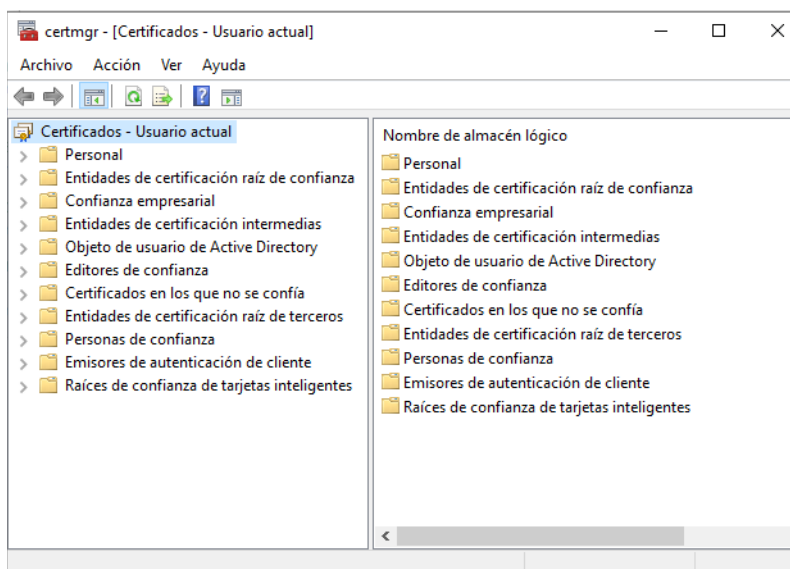
### 3. Comprueba los certificados de cifrado de archivo de "usu1"

- Puedes escribir "certificado" en el panel de control.



### 4. Comprueba los certificados de usuario personales de "usu1"

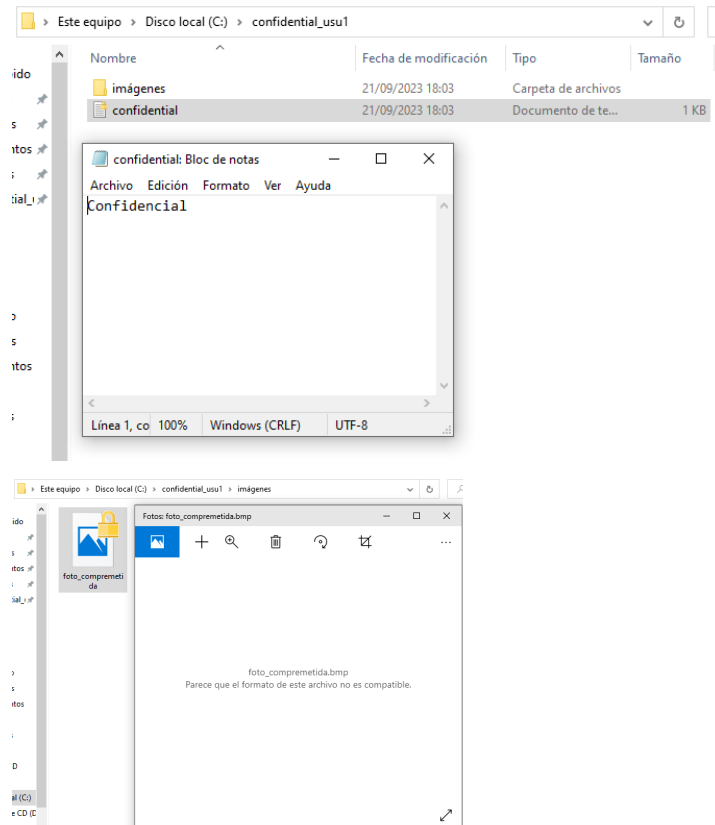
- Puedes escribir "certificado" en el panel de control.



## 5. Comprueba que puedes abrir y ver los documentos:

> confidential\_usu1/confidential.txt

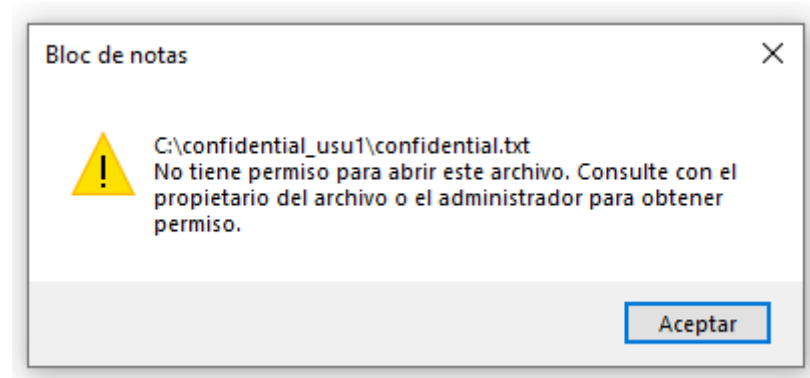
> confidential\_usu1/imágenes/foto\_comprometida.jpg

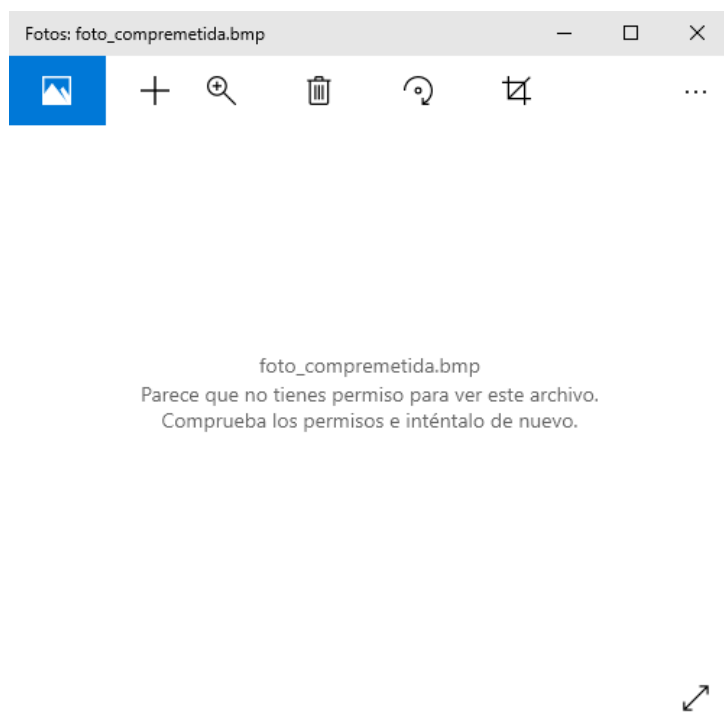


## 6. Inicia sesión con el usuario "usu2" y trata de abrir los documentos:

> confidential\_usu1/confidential.txt

> confidential\_usu1/imágenes/foto\_comprometida.jpg





## PARTE B

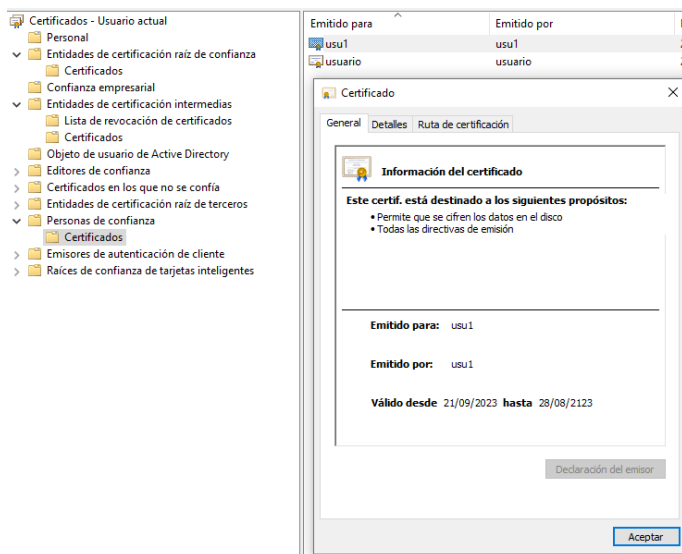
Investiga sobre como conseguir que el usuario "usu2" pueda abrir los documentos cifrados por "usu1".

Para ello, deberás exportar el certificado con clave privada y entregárselo a "usu2"

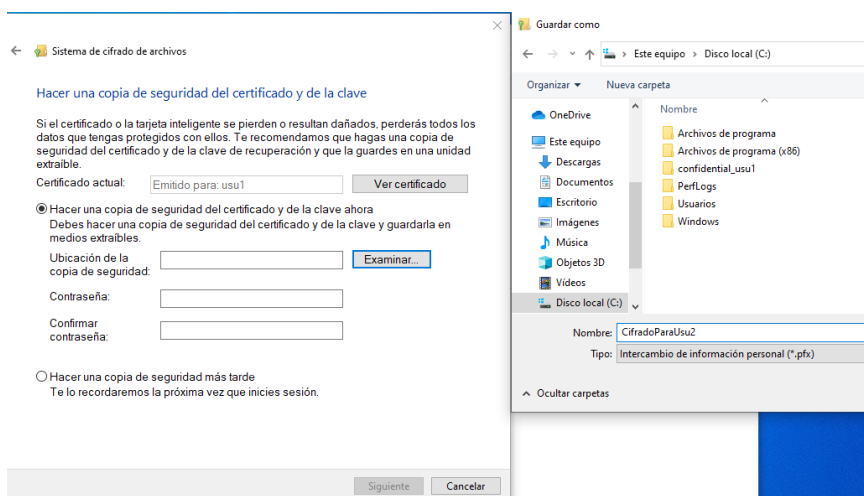
- Haz un tutorial con explicación y pantallazos de todo el proceso.

Indica todo el proceso de exportación por "usu1", importación por "usu2" y lectura de los documentos cifrados por "usu2"


### PASO 1. Abrir los certificados de usuario desde el panel de control.



### PASO 2. Hacer una copia del certificado y de la clave desde el panel de control.



### PASO 3. Elegimos la ruta de la copia de seguridad y escribimos la clave.

←  Sistema de cifrado de archivos

×

#### Hacer una copia de seguridad del certificado y de la clave

Si el certificado o la tarjeta inteligente se pierden o resultan dañados, perderás todos los datos que tengas protegidos con ellos. Te recomendamos que hagas una copia de seguridad del certificado y de la clave de recuperación y que la guardes en una unidad extraíble.

Certificado actual:

☒ Hacer una copia de seguridad del certificado y de la clave ahora  
Debes hacer una copia de seguridad del certificado y de la clave y guardarla en medios extraíbles.


Ubicación de la copia de seguridad:

Contraseña:

Confirmar contraseña:

☐ Hacer una copia de seguridad más tarde  
Te lo recordaremos la próxima vez que inicies sesión.

### PASO 4. Así se realizaría la copia de seguridad, ahora tendremos que iniciar sesión con usu2.

←  Sistema de cifrado de archivos


×

#### Se realizó una copia de seguridad del certificado y de la clave

Detalles del certificado:

Emitido para: usu1  
Emitido por: usu1  
**Expira el: 28/08/2123**

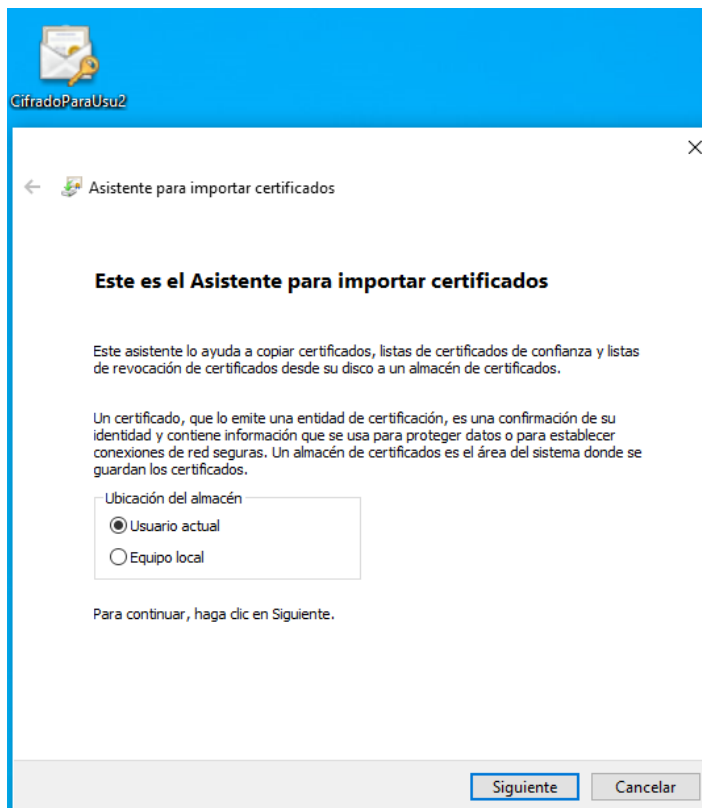
Ubicación de la copia de seguridad de clave y certificado:  
C:\Users\usu2\Desktop\CifradoParaUsu2.pfx



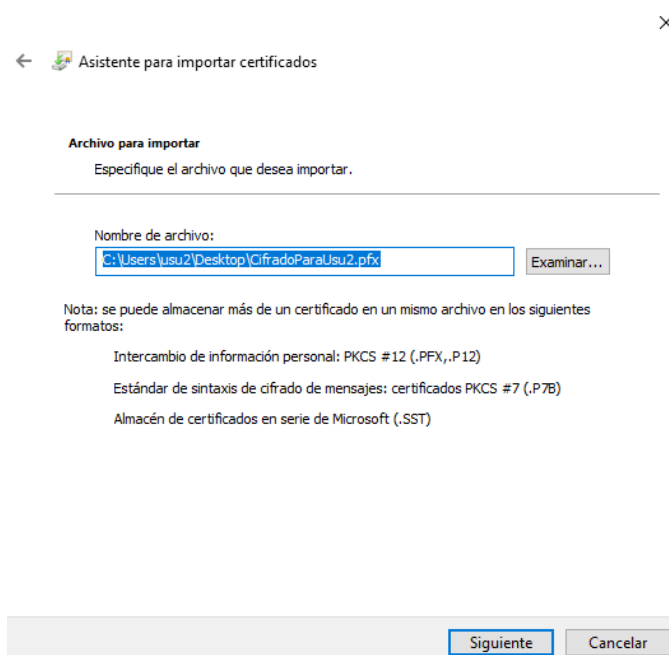
No se arriesgue a perder el acceso a los archivos cifrados. Actualice lo antes posible los archivos cifrados con anterioridad para que usen este certificado y esta clave.





## PASO 5. Una vez tengamos el certificado, lo abrimos y procederemos a su importación.




## PASO 6. Seleccionamos el certificado que queremos instalar.



## PASO 7. Ahora escribimos la clave privada para descifrar el certificado.

  Asistente para importar certificados



**Protección de clave privada**  
Para mantener la seguridad, la clave privada se protege con una contraseña.

Escriba la contraseña para la clave privada.



Contraseña:  
  
☒ Mostrar contraseña

Opciones de importación:  
☐ Habilitar protección segura de clave privada. Si habilita esta opción, se le avisará cada vez que la clave privada sea usada por una aplicación.  
☐ Marcar esta clave como exportable. Esto le permitirá hacer una copia de seguridad de las claves o transportarlas en otro momento.  
☐ Proteger la clave privada mediante security(Non-exportable) basada en virtualizado  
☒ Incluir todas las propiedades extendidas.

Siguiente

Cancelar

## PASO 8. Una vez finalizado, ya tendríamos acceso a la carpeta cifrada de usu1.

  Asistente para importar certificados

**Finalización del Asistente para importar certificados**

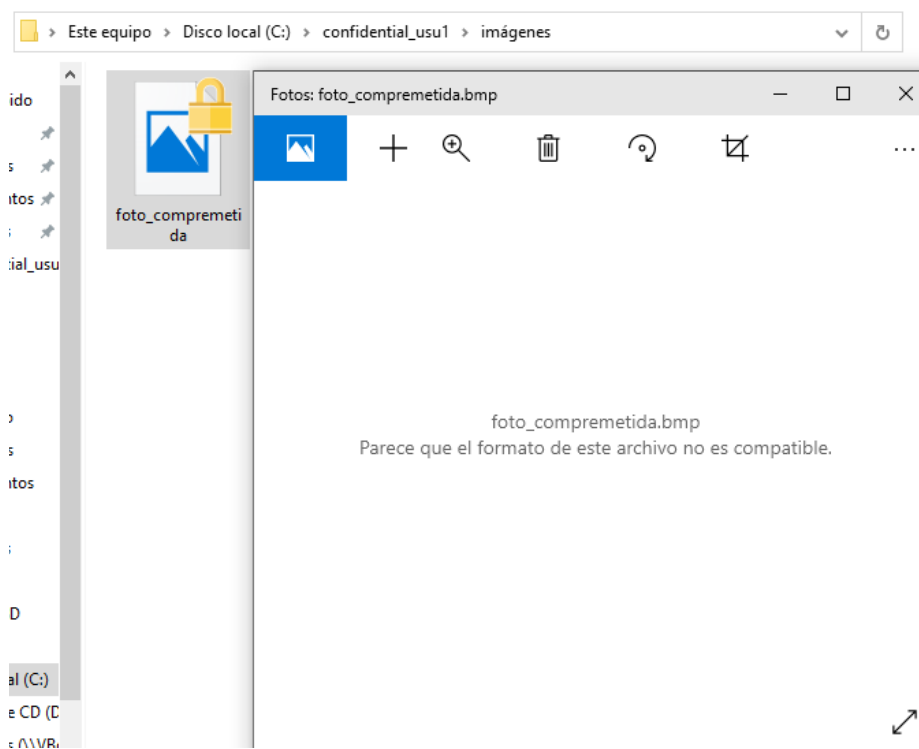
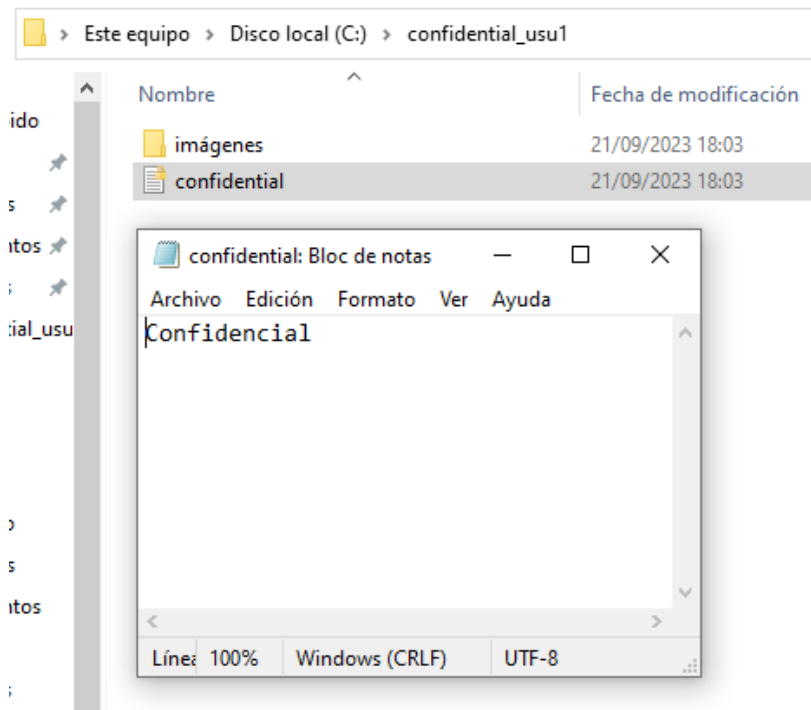
Se importará el certificado después de hacer clic en Finalizar.

Especifíco la siguiente configuración:

Almacén de certificados seleccionado	Determinado de forma automática por el asistente
Contenido	PFX
Nombre de archivo	C:\Users\usu2\Desktop\CifradoParaUsu2.pfx

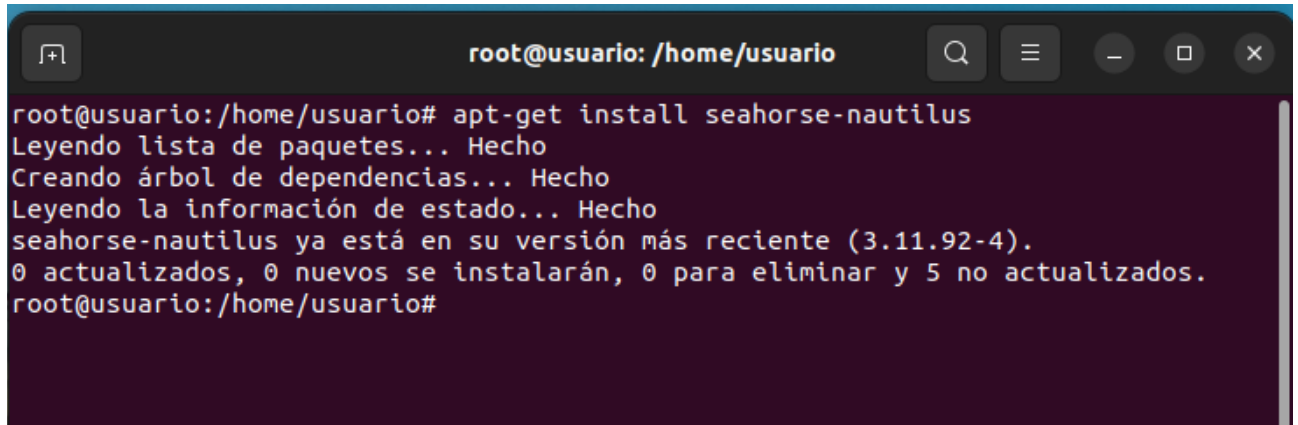
Finalizar

Cancelar



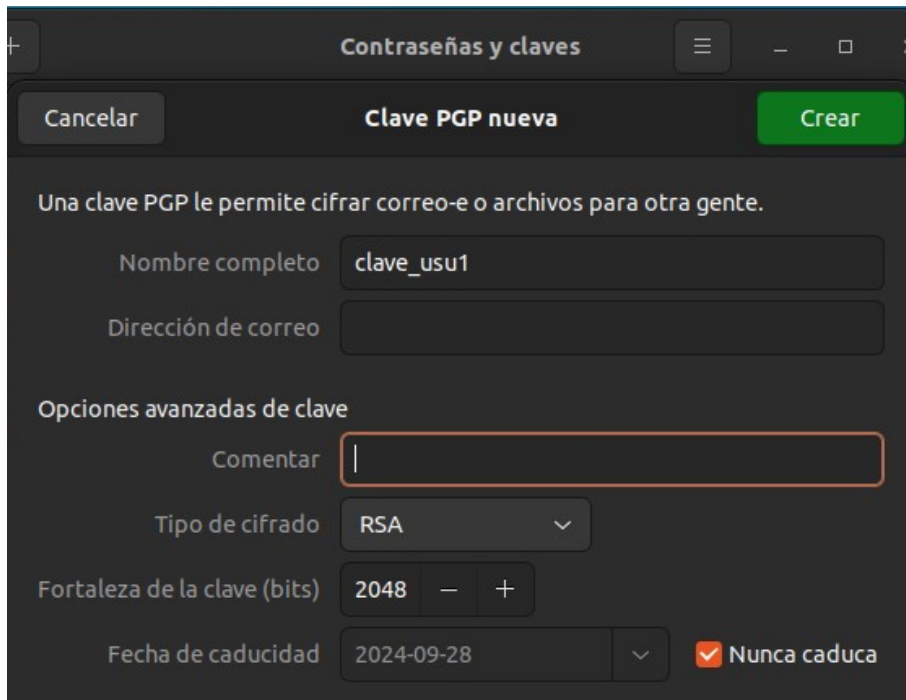
## PARTE DE LINUX

### PASO 1. Instala el paquete "seahorse-nautilus".



```
root@usuario: /home/usuario
root@usuario:/home/usuario# apt-get install seahorse-nautilus
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
seahorse-nautilus ya está en su versión más reciente (3.11.92-4).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 5 no actualizados.
root@usuario:/home/usuario#
```

### PASO 2. Accede al gestor de contraseñas y claves de Ubuntu.



Contraseñas y claves

Cancelar Clave PGP nueva Crear

Una clave PGP le permite cifrar correo-e o archivos para otra gente.

Nombre completo

Dirección de correo

Opciones avanzadas de clave

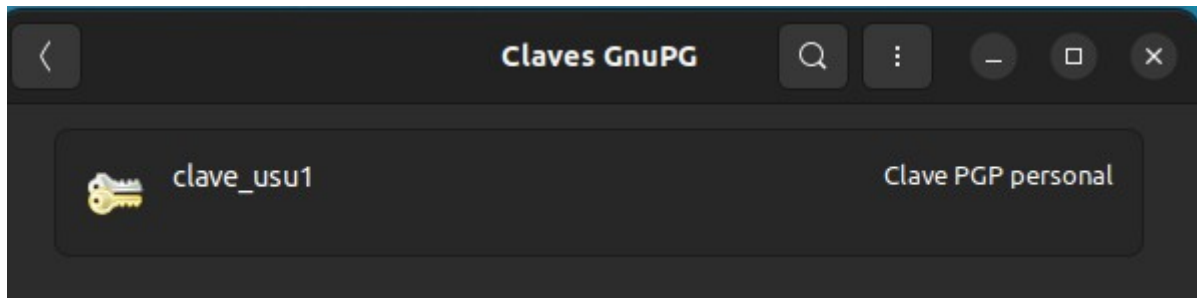
Comentar

Tipo de cifrado

Fortaleza de la clave (bits)  - +

Fecha de caducidad  ☒ Nunca caduca

**PASO 3. Crea una nueva clave PGP "clave\_usu1" con contraseña "abc123."**



**PASO 4. Crea la siguiente estructura de carpetas y documentos en el escritorio:**

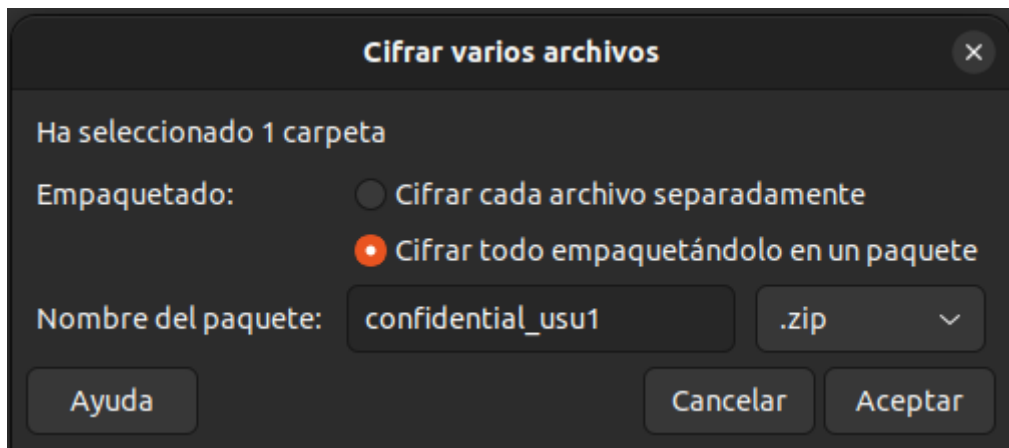
-> Carpeta "confidential\_usu1"

|  
|-> Documento "confidential.txt" con texto guardado

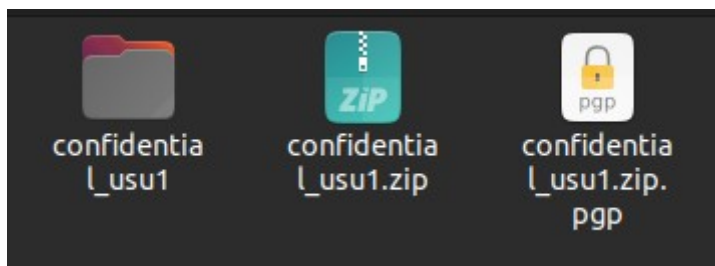
|  
|-> Subcarpeta "imágenes"

|  
|-> Imagen "foto\_comprometida.jpg"

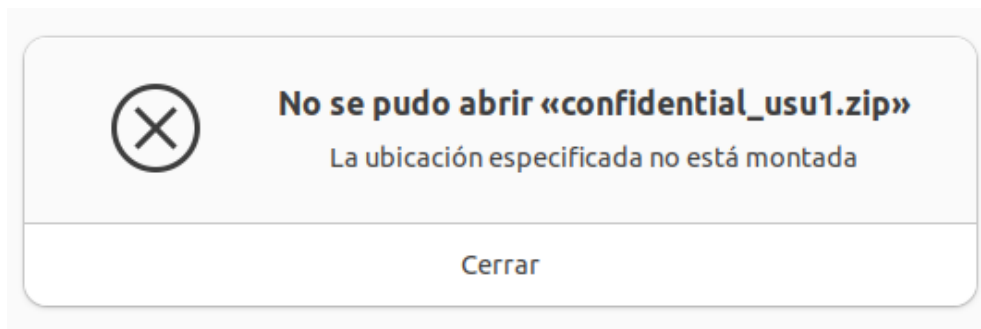
**PASO 5. Cifra la carpeta usando la clave PGP "clave\_usu1". Para ello selecciona la opción de cifrar en un único paquete.**



**PASO 6. Muestra el fichero .pgp creado.**



**PASO 7. Inicia sesión con otro usuario "usu2" e intenta descifrar el fichero .pgp.**



**PASO 8. Vuelve a iniciar sesión con el usuario original "usu1" y descifra el fichero .pgp.**

